



**Document Number:** NASPO IDPV 009

**Date Issued:** January 25, 2011

---

## **DRAFT REPORT**

**of the  
3rd Meeting  
held at  
LexisNexis, Alpharetta, GA  
January 19-21, 2011**

**for the Development of an American National Standard to establish  
Minimum Standards for Proof and Verification of Personal Identity**

---

### **Table of Contents**

[Introduction and Summary](#)

[Overview of Prior IDSP Work](#)

- 1.1 [Opening, Welcome and Anti Trust Statement](#)
- 1.2 [Approval of Agenda](#)
- 1.3 [Approval of 2nd Meeting Report](#)
- 1.4 [Roll call of the IDPV Consensus Body](#)
- 2.1 [Overview of the ISO Standard Development Process – Working Draft](#)
- 3.1 [Report of the Authoring Committee](#)
- 4.1 [Report of Test and Evaluation Committee](#)
- 5.1 [Brief Report on the Project Status](#)
- 6.1 [Purpose, Organization & Protocol for Workshops](#)
- 6.2 [Workshop 1](#)
- 7.1 [Workshop 2](#)
- 7.2 [Workshop 3](#)
- 7.3 [Workshop 4](#)



8.1 [Report on Outcome of Workshop Activities](#)

8.2 [Breakdown & Allocation of Responsibilities for Completion of Outstanding Work Items](#)

8.3 [Timelines and Milestones](#)

9.1 [Location, Length and Date of Next Meeting](#)

[Review of Actions](#)

[Committees](#)

[Motions](#)

[EXHIBIT 1](#) – NASPO Anti-Trust Statement

[EXHIBIT 2](#) – List of Attendees

[EXHIBIT 3](#) – Approved Agenda

[EXHIBIT 4](#) – Explanation of a Working Draft

[EXHIBIT 5](#) – Authoring Committee Report

[EXHIBIT 6](#) - Project Leader Report

[EXHIBIT 7](#) – Workshop 1 Brief

[EXHIBIT 8](#) – Workshop 1 Worksheets

[EXHIBIT 9](#) – Kim Little Report



## **Introduction and Summary** ([Back to Top](#))

The three day meeting reported in this document was the third meeting of the body formed to reach consensus on an American National Standard for Proof and Verification of personal identity. The meeting reported was attended by 23 persons representing 20 organizations all involved directly or indirectly in the issue of identity risk management and identity fraud countermeasures.

Major outcomes of the meeting included :-

- Report of the Authoring Committee.
- Report of the Test and Evaluation Committee.
- Consensus on the need for a requirement specification methodology
- Formation of a Quantification Committee.
- Formation of a Trust Framework sub-Committee
- Formation of a Privacy sub-Committee
- Formation of a Best Practices sub-Committee
- Formation of a Definition sub-Committee
- Formation of a Legal and Legislative sub-Committee
- Better understanding by all of privacy issues
- Division of activities for sub-groups
- The location and date of the next meeting.

## **Overview of Prior IDSP Work** ([Back to Top](#))

Prior to the start of the main meeting the Project Leader, Graham Whitehead and a group of attendees who had participated in the initial work of the IDSP project provided an explanation of the basis of conclusions and recommendations resulting from the ANSI/BBB IDSP and NASPO ID-V Project that culminated in the initiation of this standard development project.

## **Agenda item 1 – Organizational Matters**

### **1.1 Opening, Welcome and Anti Trust Statement** ([Back to Top](#))

The meeting was opened by the Executive Director of NASPO Mr. Michael O’Neil. Mr. O’Neil then welcomed the group to Alpharetta and thanked LexisNexis for hosting the meeting. Following his welcome, Mr. O’Neil read the NASPO Anti-Trust policy, [Exhibit 1](#) and stressed the need for all attendees to avoid engaging in any activities of an anti-trust nature and to leave the meeting if such activities persist. Mr. O’Neil then invited all attendees to introduce themselves. The list of attendees and their affiliation is shown in [Exhibit 2](#).

### **1.2 Approval of Agenda** ([Back to Top](#))

The Agenda for the meeting is shown in [Exhibit 3](#). **A motion to modify the agenda to one Workshop on methodology on Day 1 with 3 workshops on Privacy, Trust Frameworks**



**and Best Practices on Day 2** was made by Tom Lockwood, seconded by Dan Combs and with no objections or abstentions was approved by all.

A second motion was made by Tom Lockwood, seconded by David Haas **to use the outcome of the workshops to refine future plans for the development of the standard.** With no objections or abstentions, the motion was approved by all

#### 1.2.1 **Appointment of a Action Item Committee** ([Back to Top](#))

At the request of the Chairman, Dennis Kallelis and Kimberly Little agreed to make note of actions resulting from the meeting and report those actions under agenda item 8.1.

#### 1.3 **Approval of 2nd. Meeting Report** ([Back to Top](#))

Comments on the 2nd Meeting report were provided NIST. In Section 3.1 under the heading Testing and Evaluation the representative of NIST present at the 2<sup>nd</sup> meeting noted that NIST had raised an objection to the development of a Test and Evaluation Plan. In accordance with the request made by NIST, Section 3.1 of the 2<sup>nd</sup> meeting report under the heading “Testing and Evaluation” was revised to include the following wording : *“NIST did not support establishing this group until such time the requirements were well defined and a complete draft was available to review”*.

A motion **to approve the meeting report as amended** was made by Jack Barnett, seconded by David Haas. There were no objections or abstentions and the motion was approved by all. The approved final version of the 2nd meeting report will be available for download at [IDPV 2nd Meeting Final Report](#)

#### 1.4 **Roll Call of the IDPV Consensus Body** ([Back to Top](#))

The Chairman proposed using the list of attendees at this meeting as the Consensus body. There were no comments or objections to this proposal.

### **Agenda item 2 – ISO Standard Format**

#### 2.1 **Overview of the ISO Standard Development Process, Working Draft** ([Back to Top](#))

Mike O’Neil explained the purpose of a Working Draft, that it is an internal document for the working group and that it will be edited and revised through the “Comments” process. He went on to explain that the comments review process is a consensus process and how the comments can be documented using the ISO comment format. Everyone in the working group has the opportunity to comment. The sheet shows, concerns, any proposed changes, any disputes and how they are resolved and then the document can be revised prior to release for public review. Mr. O’Neil noted that the results of these two days of workshops should go into the working draft to be further refined and reviewed by the working groups appointed by the consensus body.



The group agreed to use the ISO format and comment tools. This works well with ANSI requirements and with any potential of moving from an American to an ISO standard. The presentation made by Mike O'Neil is shown in [Exhibit 4](#).

### **Agenda item 3 – Authoring Committee report**

#### **3.1 Authoring Committee actions to date - Dan Combs** ([Back to Top](#))

Dan Combs reported that although there was not a draft document produced by the group they had nevertheless been working hard. There had been weekly teleconferences with a considerable amount of documentation circulated by email and included on the IDPV Wikidot website. The work had helped in defining the scope of the standard.

##### Scoring

There had been discussion of a scoring system, originally suggested by Garland Land. Ted Sobel proposed that the term weighting be used rather than scoring. This led to a discussion on using common definitions to concur with the work of other groups.

##### Privacy

Another topic of discussion had been Privacy and FIPPS which was considered a key issue that must be met throughout the standard.

##### Trust

As people need to be able to be trusted they will need assurance that the standard is being implemented properly in a trustworthy process.

##### Legislative issues

This was a bigger issue than first appreciated. There is a lot going on at all levels of Federal, State and local government.

Output of the authoring committee had given clarity, but it was still individual clarity and it was anticipated that shared clarity would come from the Workshops over the next two days.

A copy of the presentation made by Dan Combs is shown in [Exhibit 5](#).

### **Agenda item 4 – Test & Evaluation Committee Plan** ([Back to Top](#))

#### **4.1 Report of the T & E Committee – Kim Little and Dennis Kallelis** ([Back to Top](#))

For their initial work, Kim and Dennis reported that the team had concentrated mainly on government use, using DMV's and made some reference to Vital records. The reason for concentrating the initial work on DMV's was to utilize the skill set of team members. They had posted the information through the Secretariat. John Biccum commented that at this time they were not comfortable with public access to their work. Questioned whether the work was secure if it was added to the Wiki, Dan Combs pointed out that access to the Wiki was by invitation only, but that did not exclude those that would use the identity of invitees to access the pages. Kim



offered to share vital record data after the meeting. The team looked at the methodology already being used by agencies and found some overlap, but individual agency requirements differ so the procedures do too.

The team noted that they needed to add members to their committee to do detailing and future work. Deborah Kobza volunteered to join the team.

A motion was made that information distilled from the report of this committee be released through the Secretariat with restricted access to the consensus body. John Biccum further amended the motion to **share collected data via the Secretariat with limited distribution and the Secretariat use appropriate procedures and markings based on 'need to know'.**

The amended motion made by John Biccum was seconded by David Haas and with no negatives or abstentions was accepted.

Tom Lockwood referenced the draft T&E plan that had been circulated on December 21, 2010 and noted that comments on the draft had been received from NIST. It has been acknowledged that NIST did not agree to this work at this time. The comments had been received by the Secretariat and forwarded to the T&E team. A response has been written and circulated within the team, but not yet forwarded to NIST.

Garland Land asked whether the team had identified the issues being confronted in the comments and whether the standard was meeting those issues. Answer was affirmative. There was discussion on whether the comments and responses should be seen by all the group, but as this is still a draft it was decided that this was not necessary and the team should send their responses to NIST.

A motion that **the consensus group direct the T&E team to send their responses to NIST comments on the T&E plan to NIST.** The motion was made by Dan Combs, seconded by Jack Barnett. Discussion resulted in an amendment to the motion, made by John Biccum, seconded by Tom Lockwood that the motion **reference that the plan was a concept plan at this time.** There were no objections or abstentions and the amended motion was accepted

A further motion was made by Jack Barnett, seconded by Dan Combs, **that the Concept T&E Plan as presented on December 18 and circulated on December 21 be approved.** The motion had one abstention (not in room to hear previous discussion), no objections and was accepted.

Garland Land posed the question of whether we know what the fraud problems are that agencies need to deal with. Presently most agencies have guidelines, but no formal need to adopt them. It is hoped that there will be a change from guidelines on processes, as presently used, to the standard, which would have all issuers being on the same understanding. John Biccum noted that there are multiple layers of checks to check documents, people and processes, and binding of documents to people. There followed a discussion on the need to eventually be proactive in reaching out to issuers and agencies, to look at their processes.

Garland was asked to look at making a motion on the topic. However, the topic was held over for Lunch break.



There was a continuation of the discussion initiated by a question from Garland Land on why are problems happening and what are we addressing?

Attendees commented that We are looking for a uniform standard process for identity verification and proofing which will be used by trusted entities. We probably cannot identify all the issues. If people understand the underlying fraud they can relate to the standard and identify the relevant items to request.

It was considered that some of the data from the original IDSP work needs reviewing and updating. The Secretariat was asked to evaluate the existing material and refresh as necessary.

Garland Land made a motion **that the secretariat review the previous current fraud scheme issues. Then the major government and private agencies that produce or receive documents for identity proofing should be contacted to identify their major fraud and identity issue. These issues are to be documented, and shared with the drafting teams to use as baseline. Action to be owned by the secretariat and the drafting team.** The motion was seconded by Ted Sobel and with no objections or abstentions the motion was accepted.

## Agenda item 5 – Project Overview

### 5.1 Brief Report on Project Status ([Back to Top](#))

There was no additional report on the work within the actual project as the current status had been covered in the reports of Agenda items 3 and 4.

It was noted that there is intention to cross link this standard with other IDPV efforts, such as the ITU-T effort and corresponding ISO 29115 Entity Authentication effort and work on going by the American Bar Association (ABA).

Also noted was consideration of changing the anticipated delivery dates of the standard as part of the T&E group Success Assurance considerations, but that the results of the workshop would help determine the need for any changes.

It was announced that the project now had confirmation of participation from the US Postal Service, AAMVA, and CBN.

Graham Whitehead noted the input into the authoring group from Patrick Curry of the BBFA (British Business Federation Authority). Patrick reinforces that the IDPV standard is relevant to the international work being carried out and that there is overlap with other activities too. He stressed the importance of looking for cooperative moves. He urged that the team look at this work with an international perspective. The presentation made by IDPV Project Leader is shown in [Exhibit 6](#).

## Agenda Item 6 – Workshops

### 6.1 Purpose, Organization & Protocol for Workshops. ([Back to Top](#))



Changes to the Workshop structure as presented in the draft agenda were proposed. The work of the authoring committee had shown the need for the development of a methodology for specifying the requirements for identity verification. As an introduction to Workshop 1, Graham Whitehead provided the brief shown in [Exhibit 7](#). He described the need for removal of Suspicion rather than verification of identity. Graham proposed that using a set methodology would lead the group to a clearer specification of requirements and consequently the proof and verification process to be used. At this time Graham proposed that the process be independent of Levels of Assurance. From input of other groups it seems that Levels of Assurance does not have common acceptance. He thought that being independent of levels, using fraud and impact as the base, entities or nations could have annexes relevant to their situation. There was a two Part framework. Part 1 of the [framework](#) identified the functions for the specification of information requirements which would lead ultimately to the removal of suspicion and acceptance or rejection of the asserted identity in Part 2 of the framework.

### **Workshop 1 – IDPV Methodology** ([Back to Top](#))

Points made by the presenter and comments made during the briefing shown in Exhibit 7 emphasized that:

The Removal of suspicion process is based on

- a. Not increasing trust, but decreasing distrust
- b. When people start a relationship, they start at a position of distrust
- c. The process is an incremental removal of suspicion
- d. “Buckets of fraud” –
  - Verbal assertion fraud
  - Borrowed credential fraud
  - Identity document fraud
  - Credential issuance fraud - there are 37 different ways that you can alter, tamper with a credential
  - Imposter fraud
  - Original identity fraud

The process focuses on context

Assesses the impact of the fraud

Establishes the symptoms of fraud for removal of suspicion

Provide knowledge on what evidence will be needed

There are 7 steps to the process – see

1. Identify Types of Fraud
2. Identify impact
3. Rank Impact of Fraud – low Medium High
4. List symptoms of fraud for high category items
5. List detection techniques for symptoms of high fraud impact
6. Spec Evidence or info required to enable detection techniques
7. Specify Info to be disclosed to assert unique identity



The workshop was to be based on this methodology to see whether it is workable, needs refining or needs re-thinking to be used as the overall IDPV framework. Graham considered that the group should use this method itself if it was to be 'preached' to others. The worksheets used for the Workshop 1 exercise are shown in [Exhibit 8](#).

There would be three groups, with a leader in each – Kim Little, Dennis Kallelis and John Biccum to each have a group. Role playing as the Director of Identity Risk Management of the DMV of Utopia and using the 7 steps on above (page 1 of the worksheet) the team would discuss and rank the questions on the following pages. The groups had one hour for discussion. Results were as follows:

Group 1 - John Biccum – need clarification of who's risk we talking about.

Table 1 – #1, no problem, #6 out of scope, all others important

Table 2 – question of potential impact on whom?

Table 3 – only looked at High category

Steps 4,5, and 6 discussions covered surveillance, multiples at one address, single agent request, data profiling, viable rules, detection, insider fraud

There was a question raised regarding whether insider fraud was in scope – Yes. The standard could also reference a standard that covers that, if available.

Group 2 - Dennis – considered that the tables had the answers in them already. Thought that role playing was good way to help figure out how the different groups assess identity risk. The group considered the wording too complex, needed to be simplified.

Group 3 - Kim – It was a tool that helped uncover things that would not have been thought of otherwise.

Following re-assembly of all participants further discussion lead to the following comments and observations:

There was discussion on the need, or not, for a method to create the draft document, with the consensus being that there has to be a methodology to make it work. Comments included:

- There had to be an analysis of risk in the system and that needed a methodology.
- A risk based tool needed.
- The standard needs a methodology.
- It may be necessary to simplify it.
- Mitigation is what we are doing.
- May need to fix on the basic structure of what documents are required.
- A good tool and we should use this tool to help test the standard once it is written.
- Exactly what is the standard going to say? Do these five things, or go through these five steps?
- Using the HIPAA example, people pick the simpler requirement.
- Are we teaching people to fish or are we handing out fish?
- This is how you fish is the goal. We might have to help people fish in some cases and produce examples for them to follow.
- We are specifying methods to validate information.
- Eliminate item 7 from the proposed methodology.
- Is the method was for the working group or for the standard for trusted identities. Response – Both.



- Use the methodology to write the standard and then follow on with method for fraud breakdown.

A motion was made by Dan Combs, seconded by Ted Sobel that **we have a risk based methodology tool to develop the standard.**

With no objections or abstentions, all voted to accept the motion.

A second motion was made by John Biccum to **use the existing straw man document provided by GDW as a starting point to develop a methodology.** This was seconded by Anna Slomovic and with no objections or abstentions was approved by all.

## Day 2

### Agenda item 7 – Parallel Workshops ([Back to Top](#))

The original intent for Day 2 was to again split into 3 groups and work three different topics – privacy, trust framework and best practices. There was discussion on whether it would be more efficient to have two groups, one on trust frameworks, the other on best practices and then join together to relate privacy to the two topics. After further debate on the options, Tom Lockwood made a motion, seconded by Jim Kragh, that **the group break into the three groups used on the previous day for one hour in order to further refine comments and concerns on the outcomes of Workshop 1 in anticipation of forming a Quantification Group** (to further advance the methodology based upon the framework presented in Workshop 1). Without objections this was accepted by all. As a result, the same 3 groups re-formed and deliberated further on the findings of Workshop 1.

Dennis Kallelis summarized the results of further deliberation by his group as follows:

- 1- Results/goals should drive the methodology. Method needs to be tied to levels 1,2,3,4 .use established standards.
- 2- Each community needs to do a risk based analysis to get their levels to 1,2,3,4
- 3- Each community needs tools and processes to get to their level of certainty.
- 4- Common language and scoring across communities to ensure a level of understanding between different communities. Communities were the issuing authorities.

Feedback is needed between communities to strengthen initial documents produced by communities. The methodology should result in one of the 4 levels

Kim Little made the presentation shown in [Exhibit 9](#) and proposed an amendment to the methodology steps.

Risk is on relying party and then the issuing party needs to review the risk to that entity. The consensus body needs to have a deliberate understanding that we are shifting much of the activity from 'positive identification' to 'negative identification' or 'removal of suspicion'.

John's group looked at Step 1 re: fraud or threat types. They considered that types 1-5 as possible but #6 – original identity fraud may be a challenge. Looking at the fraud list they looked at Table 3 and agreed that communities need to work through risk analysis and their existing controls to the needs of risk mitigation.



The three groups together discussed

- Need to understand communities better
- Who is suffering the risk?
- Universe is anyone who may rely on their credential
- Should consider insider fraud, abusing internal privileges
- No controls anywhere that look at whole manufacturing process.
- Group recognizes that some things need further clarification.
- How wide do we make the scope of the standard?
- Need to detail Step #1
- Standard should incorporate by reference a process to reach that requirement, not expand within the standard
- Need to add 'forged document' between 2&3
- Risk is probability combined with consequences.
- What is risk to the organization making the decision, and what is the risk to other organizations based on that previous decision.
- Evaluate the needs of the community via risk assessment done by each community.
- Other definitions of these frauds already out there that should be noted and referenced
- Present standard is an existing document. Need to define its edges and reference adjoining edges.
- Need to look at neighbours and international standards. Need a clean edge, not any gaps or overlaps.

### **There followed 2 demonstrations.**

Dennis Kallelis demonstrated the document authentication system developed by L11D  
Kim Little demonstrated the LexisNexis methodology for assertion of identity using publicly available information.

Motion by John Biccum to amend the agenda to have more time for discussion on Table 1-Fraud, seconded by Graham Whitehead

Discussion followed, no vote.

Tom Lockwood made a further motion **to revise the agenda to allow discussion on data mining until 3.00pm and then have breakout groups work until 6.00pm.** Motion seconded by Marc Aronson, one No vote, no abstentions, so motion carried.

Looking at Table1 – Fraud Threats. It was thought that a matrix using Techniques in the rows and Outcomes in the columns would simplify the picture. (see [Slide 10](#) of Exhibit 9)

We are looking at threat analysis for the techniques used for the creation of a false identity. Ted Sobel and Kim worked on the table in real time.

It was decided that furthering this work should be done by a Quantification committee. This committee would include Ted Sobel, Kim Little, Dennis Kallelis, Jeff Quarrington, Graham Whitehead, David Brown and Ray Philo.

Looking at the 3 workshops as originally planned, and appreciating a time constraint on Anna Slomovic a new motion was made by Tom Lockwood that **all people present remained together for Anna to share information on privacy and then have splinter groups for the remaining**



**two topics.** Anna Slomovic seconded the motion and with no objections or abstentions the change was accepted by all.

### **Workshop 2 – Privacy Considerations** ([Back to Top](#))

Anna spoke on the importance of considering privacy throughout the standard. She circulated a copy of Draft National Strategy for Trusted Identities in Cyberspace - Appendix C – FIPPS Fair Information Practice Principles.

- There is a need for transparency from the proofer.
- There needs to be an option for resolution or dispute by the issuing body. The resolution must be developed and explained.
- There should be a method of redress
- Reference could be made to the FIPP's agreement.
- Privacy should not be an appendices, it should be in the standard
- There needs to be a decision on 'should' or 'shall'
- It should be auditable

During Anna's presentation there was time for questions to be raised. Some of the issues to be addressed included

- Text in standard should say you must comply with your local jurisdictional privacy laws.
- Talk on re-dress and appeals. Ted gave good words from DHS on these items.
- Should this be a "must" or a "should" in this standard. "Should" shall be used.
- Warning and caution messages on standards.
- In the body of the standard you shall follow the FIPPS.
- Mandatory verses Elective.
- Difference between "required required" and "optional required".
- May need to make FIPPS voluntary. Government has to handle as they are regulated. There are Privacy officers in the government.
- There are people that interpret FIPPS in different ways.

The authoring committee will spin-off a group to create the standards language associated with privacy and also serve as an evaluation body for the other groups. This Privacy sub-committee will also work directly with the Secretariat. This subcommittee will be chaired by Anna Slomovic

Dan Combs proposed that the group should give Anna and her committee the right to develop privacy principles for the standard. Agreed

Looking at the remaining two workshop topics, Trust Framework and Best Practices it was decided that the group remain together and have one meeting and concentrate on the Trust Framework.

### **Workshop 3 - Trust Framework** ([Back to Top](#))

Discussion points were:

- Need trust in the system as well as in the credential
- Issuers need to know they can rely on the credential
- Need to identify and credential the provider
- Some things they must, and must not, do



- May be possible to audit the credential provider
- Need to consider state laws and legislation
- Need a system that would allow interplay between agencies
- Trustmarks could be used as a certification
- Could there be levels of trustmarks?
- Trustmarks are used within industry
- Could industry trustmarks such as those of AAMVA or ANSI be used?
- Would trustmarks be with or without a seal?
- How to establish such criteria within the standard?
- Need to run the methodology to check feasibility
- Maybe write the criteria, but not designate how it can be done
- Use attributes similar to NASPO, ISO etc.
- ISO conformity already exists
- Need to look at NPO, Commerce, Kantara
- Work with these entities
- Existing trustmarks should be referenced within the standard
- Need to decide whether the current outline addresses this adequately, whether there should be separate sections or not, and if not, how it is incorporated into the sections.
- Need a framework for work within communities
- This could relate to the agency and the document. There can be two different scores for the document and the agency
- Should there be a sub-group looking at trustmarks?
- Can we expect communities to develop criteria and benchmarks
- Will this fit into the document timeline?
- The standard can only give direction, cannot dictate levels to industry
- Need a list of communities to work with
- Need to review what is in and out of scope of the standard
- Need to work with the quantification group.
- This leads to a schema for a value of trust

A motion was made by Ted Sobel, seconded by Jeff Quarrington **that a Trust Framework sub-group of the Authoring Committee be formed.** With no objections or abstentions the motion was accepted by all

Trust Frame Work subgroup of the writing committee to:

- work with the quantification group and other edge groups.
- have meetings between certain communities and organization to build out the answer to these questions for these groups to build out the trust frame work that shall be trusted between communities which includes how it shall be used, and how it shall be detailed in text.
- expect that the various communities shall develop their trust work frame and marks
- come back with what is in scope and out of scope items.

A further motion was made by Dennis Kallelis, seconded by Dan Combs to adjourn the meeting. With no objections or abstentions the meeting closed at 5.50pm.

### Day 3



## Agenda item 8 – Summary of Action items

### 8.1 Report on Outcome of Workshop Activities ([Back to Top](#))

Dave Brown noted that talks of the past two days had covered a considerable amount of work. The outcome had been the formation of several sub-groups, under the leadership of the Authoring Committee, to detail specific work items.

### 8.2 Breakdown & Allocation of Responsibilities to Complete Outstanding Work Items

Moving forward these sub-groups are:

Privacy – Anna Slomovic, a LexisNexis person (designated by Kim Little), invite Kathleen Carroll, John Biccum will look for candidate from Microsoft

Quantification - Ted Sobel, Kim Little, Graham Whitehead, David Brown and Ray Philo.

Trust Framework – not yet designated at this time

The work of these groups will be published 30 days prior to the next meeting.

Dave Brown also noted

- Work will follow ISO format
- Secretariat is responsible to be accountable to the procedures and requirements and ensure the availability of resources
- Drafting will be consistent with procedures and respond to Secretariat

Use definitions consistent with other communities – Tom Lockwood recommended a sub-committee on Definitions and Dan Combs recommended Jack Barnett to lead this work. Support was offered by Jeff Quarrington and Brian Zimmer

Reference was made to Sections in the outline with the work for the quantification team being in sections 6.2 & 6.7, privacy in sections 6.1 and 7.1 and the trust framework being in sections 2 and 8.

It should be noted that at this time there has been no consensus approval of the use of this outline. The outline being referenced was one of several offered by members of the authoring committee as a route for writing structure. It can be adapted as appropriate as the standard evolves.

It was noted that David Smedinghoff (American Bar Association, not present) had proposed that the team should also look at legislative concerns.

A motion was made by John Biccum, seconded by Ted Sobel, that a sub-group under the authoring committee be formed to look at legislative issues with Brian Zimmer as chair. Discussion resulted in the expansion of the motion to include regulatory issues. So the motion proposed was, **that a sub-group under the authoring committee be formed to look at legislative and regulatory issues with Brian Zimmer as chair**. The amended motion received no objections or abstentions and was accepted by all.



The T&E team under Dennis Kallelis and Kim Little would look at the key issue of the reality of meeting requirements and relating to outside communities. They requested additional support, especially at the phase of external interfacing.

Dan Combs noted the availability of the Wiki and proposed that Graham and Ann Whitehead should be included in those who manage the Wiki. He proposed that he show G&A the details of managing the site.

Graham Whitehead offered to have the report of this meeting available next week.

#### **Workshop 4 – Best Practices**

Ted Sobel offered points for all to consider ([Back to Top](#))

1. Best practices needs to define peer roles and responsibilities
2. Privacy – ask permission of applicant, explain redress policy and disseminate information
3. Enrolment – pre-enrolment, information collection (including biometric and biographic) and document validation
4. Data retention policy is needed
5. Data correction needs to be part of the process
6. Revocation
7. One-stop shop – additional by reference
8. Look at other groups and notify ahead of activities
9. Personnel security
10. Different rules for minors (may not be applicable to this standard) i.e. government is 18, TSA is 16, registered traveller is 12

#### **8.3 Time lines and Milestones** ([Back to Top](#))

There was a timetable approved in the meeting at the Bolger Center. Now that there is a suggestion of asking communities for feedback there is some concern about meeting those timelines.

The timeline used dates and derivatives of those dates based on a serial process that reached to February 2012 Now the work is being changed from serial to parallel. There is a need to look to the owners of the deliverables and produce an integrated project schedule The work also needs to be integrated with the T&E plan to outreach to communities. There needs to be a framework of milestones.

John Biccum made a motion to amend the scope of the T&E group to include feedback from the targeted communities. The motion was seconded by Garland Land. Discussion ended in a further amendment that **the scope for the T&E group incorporate the outreach approach proposed by the team.** This motion was made by Kim Little, seconded by John Biccum and with no objections or abstentions was approved.

Dan Combs made a motion for the Secretariat to take charge of an integrated timeline. This was seconded by Tom Lockwood. With no objections or abstentions, the motion was approved. The motion was then amended by Tom Lockwood, seconded by Dan Combs and approved by all to



read that the Writing and T&E teams work together to give an integrated timeline of milestone deliverables to the Secretariat.

**Agenda item 9 – Next Meeting**

**9.1 Location, length and date of next meeting** ([Back to Top](#))

Rather than deciding on a date at this time, it was proposed that this meeting be held 30 days after release of the working draft. A motion was proposed by Brian Zimmer, seconded by Jeff Quarrington that **the date of the next meeting be delegated to the Secretariat based on completion of the Working Draft and 30 day review period.** There were no objection or abstentions, so the motion was approved.

It was noted that it is preferred that this meeting would be no more than 3 months from now.

The final motion was to adjourn the meeting. This was made by Dennis Kallelis, seconded by Marc Aronson and approved by all.

Adjourn at 12.40pm

**Review of Action Items Agreed at this Meeting** ([Back to Top](#))

The following actions were noted and accepted :

Action Item	Action	Responsibility	Date
1	The approved final version of the 2nd meeting report will be available for download at <a href="http://www.naspo.info">www.naspo.info</a>	Secretariat	asap
2	The group agreed to use the ISO format and comment tools.	All	ongoing
3	T&E team to send their responses to NIST comments on the T&E plan to NIST.	T&E team	immediate
4	Some of the data from the original IDSP work needs reviewing and updating. Evaluate the existing material and refresh as necessary	Secretariat	Start immediate
5	Secretariat is responsible to be accountable to the procedures and requirements and ensure the availability of resources	Secretariat	Start immediate
6	Management of the Wiki site to be shared with Graham & Ann Whitehead.	Dan Combs	Start immediate
7	Formation of a sub-committee for Best Practices	TBD	Start immediate



8	Formation of a sub-committee for Quantification	Graham Whitehead	Start immediate
9	Formation of a sub-committee for Definitions	Jack Barnett	Start immediate
10	Formation of a sub-committee for Privacy	Anna Slomovic	Start immediate
11	Formation of a sub-committee for Trust Frameworks	TBD	Start immediate
12	Formation of a sub-committee for Legal and Legislative	Brian Zimmer	Start immediate

**Committees**

**Authoring Committee** ([Back to Top](#))

Chair – Dan Combs.

Team members – Abbie Barbir, Anna Slomovic, Brian Zimmer, Clayton Bonnell, Dan Covey, David Temoshok, Dennis Kallelis, Garland Land, Graham Whitehead, Kathleen Carroll, Kim Little, John Biccum, Paul Donnelly, Ted Sobel, Tom Lockwood

This committee includes sub-committees of :

Privacy – Anna Slomovic (leader) Kathleen Carroll, a LexisNexis person (not yet named), a Microsoft person (not yet named)

Quantification – Graham Whitehead, Ted Sobel, David Brown, Kim Little, Ray Philo, Dennis Kallelis, Jeff Quarrington

Definitions – Jack Barnett (leader), Jeff Quarrington, Brian Zimmer

Legislative – Brian Zimmer (Leader),

Trust Frameworks – personnel not yet designated

Best Practices - personnel not yet designated

**Test and Evaluation Committee** ([Back to Top](#))

Co-Chairs – Kim Little and Dennis Kallelis

Team members – John Biccum, Tom Lockwood, Deborah Kobza

**Motions Made (except motions on agenda changes)**

**The consensus group direct the T&E team to send their responses to NIST comments on the T&E plan to NIST. Reference that the plan was a concept plan at this time**

**That the Concept T&E Plan as presented on December 18 and circulated on December 21 be approved**

**That the secretariat review the previous current fraud scheme issues. Then the major government and private agencies that produce or receive documents for identity proofing**



**should be contacted to identify their major fraud and identity issue. These issues are to be documented, and shared with the drafting teams to use as baseline. Action to be owned by the secretariat and the drafting team.**

**We have a risk based methodology tool to develop the standard.**

**Use the existing straw man document provided by GDW as a starting point to develop a methodology.**

**That a Trust Framework sub-group of the Authoring Committee be formed.**

**That a sub-group under the authoring committee be formed to look at legislative and regulatory issues with Brian Zimmer as chair.**

**The scope for the T&E group incorporate the outreach approach proposed by the team.**

**That the Writing and T&E teams work together to give an integrated timeline of milestone deliverables to the Secretariat.**

**The date of the next meeting be delegated to the Secretariat based on completion of the Working Draft and 30 day review period.**



## **EXHIBIT 1 – NASPO Anti Trust Policy** [\(Back to Top\)](#)

NASPO intends to comply with all applicable antitrust laws. Under no circumstances will NASPO directly or indirectly be involved in conduct that leads to or implies an agreement among its members that would restrain trade and/or otherwise violate antitrust laws. Any conduct by NASPO's officers, directors, or employees that is contrary to the antitrust laws is contrary to NASPO policy. Any officer, director, or employee found in violation of this policy or the applicable antitrust laws will be subject to appropriate disciplinary action.



**EXHIBIT 2 – Meeting Attendees** ([Back to Top](#))

Meeting Attendees	Organization	eMail Address
Geoff Slagle	AAMVA	gslagle@aamva.org
Jack Barnett	American Banknote	jbarnett@abnotena.com
Anna Slomovic	Anakam/Equifax	aslomovic@anakam.com
Jeff Quarrington	Canadian Bank Note Company	jquarrin@cbnco.com
Brian Zimmer	Coalition for a Secure Drivers License	brian@idsecuritynow.org
Tom Lockwood	Consultant	thomas.j.lockwood@gmail.com
Ted Sobel	DHS Office of Policy	ted.sobel@dhs.gov
Dan Combs	eCitizen Foundation	dancombs1@gmail.com
James Kragh	Good Health Network	kragh@ghnet.us
David Brown	Intel	david.a.brown@intel.com
Dennis Kallelis	L1 Identity Solutions	dkallelis@L1ID.com
Kim White	LexisNexis	kimberley.white@lexisnexis.com
Kimberly Little	LexisNexis	kimberly.little@lexisnexis.com
John Biccum	Microsoft	johnbic@microsoft.com
Garland Land	NAPHSIS	gland@naphsis.org
Ann Whitehead	NASPO	naspo@telus.net
Graham Whitehead	NASPO	gdw@naspo.info
Mike O'Neil	NASPO	mikeo@naspo.info
Deborah Kobza	NH-ISAC	dkobza@nhisac.org
Marc Aronson	PA Association of Notaries	maronson@notary.org
David Haas	Teccocorp	david@teccocorp.com
Wai Tsang	TecSec	wtsang@tecsec.com
Raymond Philo	Utica College	rphilo@utica.edu
Patrick Curry of BBFA was on standby by phone from UK to participate in Day 3 discussions concerning possible changes to project timetable. In the event no changes were proposed and hence Patrick was not contacted to participate.		
Patrick Curry	BBFA (UK)	patrick.curry@federatedbusiness.org



**EXHIBIT 3 – Approved Agenda** ([Back to Top](#))

**Document Number:** IDPV 006  
**Date Issued:** December 21, 2010  
**Date of Revision:** January 19, 2011

---

**REVISED DRAFT AGENDA**

**Development of an American National Standard to Establish  
Minimum Standards for Proof and Verification of Personal Identity**

**Third Meeting of Interested Parties**

[LexisNexis](#)  
1000 Alderman Drive  
Alpharetta, GA, 30005

**Full-Day Meetings: Wednesday & Thursday, January 19 and 20, 2011**

8:00 am – 4:00 pm Wednesday

9:00 am – 4:00 pm Thursday

9:00 am – 12 pm Friday

**Casual Dinner: Wednesday evening, January 19**

6:30pm – 9:00pm

Vinny's, 5355 Windward Parkway

---

**Day 1**

Overview of Prior IDSP Work  
(8:00–9:00)

Graham Whitehead, Dan  
Combs, Tom Lockwood,  
Brian Zimmer, David Haas

**Agenda Item 1 – Organizational Matters**

1.1 Opening  
(9:00–9:15)

Mike O’Neil  
NASPO Executive Director

- 1.1.1. Welcome and Self-Introductions across the group
- 1.1.2. NASPO Anti-Trust Policy

1.2 Approval of Agenda (Action)  
(9:15 – 9:20)

David Brown  
IDPV Project Chairman

1.3 Approval of 2nd. Meeting Report (Action)  
(9:20 – 9:45)

David Brown  
IDPV Project Chairman

**Document:** IDPV 004



- 1.4 Roll Call of the IDPV Consensus Body (Action)  
(9:45 – 10:00)  
The Chairman will review and confirm the roster of the consensus body.

David Brown  
IDPV Project Chairman

10.00-10.15am Break

**Agenda Item 2 – ISO Standard Format**

- 2.1 Overview of the ISO Standard Development Process  
(10.15 -10.30)

Mike O’Neil  
NASPO Executive  
Director

**Summary:** The speaker will provide:  
Information on the steps involved in the drafting on an International Standard that highlights the ISO process for public and committee comment

**Agenda Item 3 – Authoring Committee Report**

- 3.1 Report of the Authoring Committee actions to date  
(10.30 -11.15)

Dan Combs  
IDPV Authoring  
Committee Chair

**Summary:** The Committee Chair will provide:  
An account of issues addressed and work carried out to date by the authoring committee

**Agenda Item 4 – Test and Evaluation Plan**

- 4.1 Report of the Test & Evaluation Committee actions to date  
(11.15-noon)

Dennis Kallellis &  
Kimberly Little  
IDPV Test & Evaluation  
Committee Co-Chairs

**Document:** IDPV 008 (IDPV Test & Evaluation Plan)

**Summary:** The Committee Chair will provide:  
The plan to date and describe how it meshes with the project plan and milestones. Time will then be devoted to the development of suitable test and evaluation criteria

**Goals:**  
The Consensus Body will amend and/or approve the T&E Plan and T & E criteria

Noon – 12.45pm - Lunch



**Agenda Item 5 – Project Overview**

- 5.1 Brief report on the Project Status  
(12.45 -1.00pm)

Graham Whitehead  
IDPV Project  
Leader/Facilitator

**Summary:** A short report on the project to date

**Agenda Item 6 – Workshops**

- 6.1 Purpose, Organization & Protocol for Workshops  
(1.00-1.30pm)

Graham Whitehead  
IDPV Project  
Leader/Facilitator

**Summary:** A series of workshop activities aimed at building consensus will be carried out over Wednesday afternoon and Thursday

**Goals:**

The workshop will aim to reach consensus on:-

1. An overall IDPV framework
2. Identification of accessible sources of identity evidence
3. Cross linking a person to available records
4. Availability of evidence of continuous use of identity
5. The feasibility of quantification of identity certainty

- 6.2 Workshop 1  
(1.30-4.00pm)

3 groups

An overall IDPV framework

**Day 2**

**Agenda Item 7 – Parallel Workshops (continued)**

- 7.1 Workshop 2

3 groups

How to incorporate PRIVACY from outset of standard development

- 7.2 Workshop 3

3 groups

Trust Frameworks

Noon - Lunch

- 7.3 Workshop 4

3 groups

Best Practices



**Day 3**

**Agenda Item 8– Summary of Action Items**

8.1 Report on Outcome of Workshop Activities (Information) David Brown  
(9.00am-10.00am) IDPV Project Chairman

10.00-10.15am Break

8.2 Breakdown & allocation of responsibilities for completion of outstanding work items John Biccum  
(10.15-11.15am) Tom Lockwood

8.3 Initial Integrated Plan of Action including a revised timeline and deliverable schedule John Biccum  
(10.15-11.15am) Tom Lockwood

**Agenda Item 9 – Plan for Next Meeting**

9.1 Location, length and date of next meeting to be discussed David Brown  
(11.15–11.30am) IDPV Project Chairman

**Agenda Item 10 – Adjournment**

10.1 Closing Remarks & Adjournment David Brown  
(11.30–12.00pm) Friday, January 21 IDPV Project Chairman



## **EXHIBIT 4 – A Working Draft** ([Back to Top](#))

What is a working draft?

A working draft is the initial draft of the standard encompassing the original concepts and principles for which the standard was proposed.

The initial working draft is not a consensus document.

The working draft is an internal document to the working group.

It will be edited and revised through the “Comments” process.

The “Comments” review process is a consensus process.

During this “Comments” process new ideas, concepts, wording and any additional revisions can be introduced and included in the draft if there is consensus by the working group.

This process allows every individual and organization to have input to the creation of the standard.

The working group will determine through a vote when the document has reached a final draft stage. At this point it may be released for public comments.

Consensus does not unanimous: some comments will accepted, some comments will be rejected, a great many will be revised and accepted through compromise.



**EXHIBIT 5 – Authoring Committee Report** [\(Back to Top\)](#)

# Writing Team Summary

Dan Combs – Team Chair



# Overview - Writing Team

Dan Combs – Chair

Graham Whitehead – Scribe

## Members at Large:

- Marc Aronson maronson@notary.org,
- Abbie Barbir  
abbie.barbir@bankofamerica.com,
- John Biccum <johnbic@microsoft.com,
- Clayton Bonnell  
clayton.bonnell@usps.gov,
- Kathleen Carroll  
KCarroll@hidcorp.com,
- Dan Covey  
dan.covey@wellsfargo.com,
- Paul Donnelly  
pauldonnelly@mindspring.com,
- Dennis Kallelis, dkallelis@L1ID.com,
- Garland Land, gland@naphsis.org,
- Kim Little  
kimberly.little@lexisnexis.com,
- Tom Lockwood  
thomas.j.lockwood@gmail.com
- Peyton Old, peytonu@attglobal.net,
- Anna Slomovic  
aslomovic@anakam.com,
- David Temoshok  
david.temoshok@gsa.gov,
- Richard Varn [rjmvarn@msn.com](mailto:rjmvarn@msn.com),
- Kim White  
Kimberly.white@lexisnexis.com,
- Ann Whitehead, naspo@telus.net,
- Brian Zimmer, brian@idsecuritynow.org,



## Overview - Efforts to Date

- Established communication exchange mechanisms
  - Organized and conducted weekly teleconferences on priority issues
  - Established Wiki to support exchange and documentation of ideas, issues, and shared communications
  - Collaborated weekly with the Evaluation Team
- Conducted extensive review, discussion, and dialog across the breadth of the proofing and verification process consistent with the scope
- Reviewed organizing principles relating to:
  - Understanding and defining key milestones, activities, and dependencies.
  - Management and execution on work activities
  - Next steps to address functional program and process issues
  - Ordering elements for the creation of outline of the draft standard.
- Identified multiple functional program and process issues clustered into functional areas:
  - Process phases and best practices
  - Quantification of data relating to risk, assurance, and certainty
  - Definitions of standard terms and references
  - Privacy and Fair Information Practice Principles
  - Trust Framework practices and principles
  - Legislative Issues & Concerns



Lets discuss in more detail ...



# IDPV Outline

**1. Scope –**

**2. Conformance –**

**3. Normative References –**

**4. Terms and Definitions –**

**5. Symbols and Abbreviated terms –**

**6. Normative Criteria (What)**



# IDPV Outline

## 6.1 Privacy

Privacy principles

Requirements for assertion and proof, existing laws, privacy community norm.

## 6.2 Assurance and Certainty

Requirements review and analysis of sample and reference data and their quantification.

Requirements for a scoring system based on viable, fundamental evidence linking a person to record

Record attributes such as timeliness, accessibility, assurance, trust, consistency, continuous use, availability, and machine and electronic read and authentication

Requirements for consistency / equivalency within and across in-person and remote processes

Transparency of criteria

## 6.3 Proofing and Verification Process Phases

Requirements derived from best practices and processes within identity proofing and verification communities and document "as is metrics"

Defined core process phases (assertion, discovery ...)

Define supporting documentation, block diagrams, and process flowcharts (inputs, outputs, decision points, criteria for decision).

Requirements for in-person and remote



# IDPV Outline

## **6.4 Special situations/issues**

Requirement to accommodate inability for certain demographics to comply for unique, but repeatable criteria or process (for example ADA, disaster with total loss of records).

## **6.5 Record Keeping**

Required record gathering and retention,

## **7. The Standard – (Required How)**

7.1 Privacy

7.2 Assurance and Certainty

7.3 Proofing and Verification Phases

7.4 Special situations/issues

7.5 Record Keeping

## **8. Evaluation & Testing -**

## **9. Annexes –**

Guidelines for Implementation (Informative)

Birth Certificates

Drivers' Licenses



## Process Phases & Best Practices

### Issues:

- Lack of clearly defined process standards for core process phases
- Inconsistent practices within identity proofing and verification communities
- Limited best practice references, lack of inter and intra community best practices
- Technology driven identity media and authentication changes changing proof and verification models
- Ongoing and persistent threat of fraud and threat
- Sensitivity by issuers to process impacts and throughput due; individuals to concerns on privacy and exposure

### Next Steps

- Identify key best practices and processes within identity proofing and verification communities and document “as is metrics”
- Define the core process phases
- Provide supporting documentation, block diagrams, and process flowcharts (inputs, outputs, decision points, criteria for decision).
- Generate Best Practice Guidance

### Primary Area of Impact to Draft Standard –

- Sections 6 & 7



## Quantification of Data Relating to Risk, Assurance, & Certainty

### Issues:

- Diverse spectrum of reference data, diversity in choice, sources, providers, quality, and integrity.
- Large variances of trust and trust-frameworks across levels, communities, use cases; like products are valued differently and contain circular references
- ID Providers & Requirement Setters desire choice flexibility in tension with individual desire for privacy & protection
- Lack of recognized standards based equivalency of proofing and verification based on certainty.
- Ongoing and persistent threat of fraud and threat
- Inconsistent risk framework to limits participants the ability to determine relationships that works for their specific community and their particular needs.

### Next Steps

- Provide summary review and analysis of sample and reference data and their quantification.
- Create a scoring system based on viable, fundamental evidence linking a person to record
- The scoring system will consider record attributes such as timeliness, accessibility, assurance, trust, consistency, continuous use, availability, and machine and electronic read and authentication

### Primary Area of Impact to Draft Standard –

- Sections 6 & 7



# Standard Terms & Reference Definitions

## Issues:

- Several conflicting community-based definitions exist and use in community operations.
- Inconsistent use of terms and lack of semantic interoperability occurring within and across communities. Examples include phrases such as proof, assertion, verification, authentication, in-person proofing, remote proofing, relying party, issuing party, etc)
- Several bodies are concurrently defining or including identity proofing and verification definitions.
- Lack of unifying activities to harmonize definitions

## Next Steps

- Ensure definition consistency and semantic interoperability with ongoing standard and community standard bodies.
- Support potential inter-standards body working body or workshop(s) on definitions.
- Key deliverable includes a list of terms and definitions to be leveraged with this and other standards bodies.

## Primary Area of Impact to Draft Standard –

- Sections 4 & 5



## Privacy & Fair Information Practice Principles (FIPPs)

Fair Information Practice Principles (FIPPs) help protection of privacy and infringement of civil liberties through misuse and exposure of private information. FIPPs are guidelines that represent widely-accepted concepts concerning fair information practice in an marketplace collection and use personal information and safeguards to assure that practice is fair and provides adequate information privacy protection.

### Issues:

- Broad international agreement on the substance of FIPPs, different statements of FIPPs sometimes look different.
- Statutory implementations of FIPPs vary in different countries, contexts, and sectors. Multiple ways to comply with FIPPs for different types of records and record keepers. In the US, elements of FIPPs are occasionally required by law for specific classes of record keepers or categories of records.
- Private sector compliance with FIPPs principles, while slowly increasing, mostly voluntary and sporadic.
- Shortened or incomplete versions of FIPPs have sometimes been offered in the United States by federal agencies or trade associations. For example, *Notice and choice is sometimes presented as an implementation of FIPPs, but it typically falls well short of FIPPs standards.*

### Next Steps

- provide expertise and supporting recommendations to ensure adherence to privacy principles – both in specific sections of the standard and across the standard.
- Areas of particular note include requirements for assertion and proof, existing laws, privacy community norm, and inclusion of FIPPs.

### Primary Area of Impact to Draft Standard –

- Section 6 in particular and influence throughout the document.



# Trust Framework

Trust Framework define the roles and responsibilities of a particular set of participants. Trust Frameworks specify the rules that govern participation and outline the processes and procedures that provide mutual assurance between participants. Key factors include requirements for participant auditing qualifications and processes, organizational maturity, identity provider credentials and their issuance, and service provider privacy policies.

## Issues:

- Lack of trust framework limits relying parties who accept identity credentials or proof to trust the identity, security, and privacy policies of the party who issues the credential and vice versa
- Many different trust frameworks exist within the Identity Ecosystem

## Next Steps

- Ensure collaboration and coordination with national efforts supporting the development of trusted identity ecosystem including standards, practices, accreditation, and certification activities and processes.
- Consistence with those principles to support the creation of accreditation criteria which clarifies ambiguities, supports compliance or assessment, and supports establishment of criteria and guidelines.

## Primary Area of Impact to Draft Standard –

- Sections 2, 6, 7, and 8.



## Legislative Issues & Concerns

Legislative activities focused on Identity Management and Privacy are increasing at all levels of government and regulated industry. While many have the same strategic intent, several do not or the strategic intent is lost in inconsistent implementation. Additionally given several recent identity related national priorities (health care, banking, etc) additional legislation is being implemented or considered.

### Issues:

- Multiple legislative and Public Sector efforts to protect an individual privacy.
- Many of these activities are stand-alone or siloed, creating new challenges
- Implementation of state-based efforts

### Next Steps

- ensure coordination with several standards bodies currently reviewing legislative concerns and corrective recommendations to enhance trustworthiness of identity related processes.
- Identify legislative issues and concerns that might impact IDPV standard development or criteria,
- ensure visibility to legislative changes and priorities

### Primary Area of Impact to Draft Standard –

- Potential impacts to all sections

Figure 1



# Outputs of Discussions

(Please See Handouts)

## Chairman's Version

- Synthesis of the team consensus process, strategic intent, and lack of consensus
- Intent is to respect the views presented

## Key Products

- Outline of the Draft Standard
- Work Organization & Management Framework
  - Incorporates the Outline of the Draft Standard
  - Organizes expertise within common areas to resolve functional issues
- Integrated Plan of Action and Milestones



[\(Back to Top\)](#)

## Request for Clarity

- The work of the Drafting Team would benefit greatly from more **CLARITY.**



[\(Back to Top\)](#)

## EXHIBIT 6 – Project Leader Report

### 1. Progress Made on Several Fronts

- Authoring Committee
- T & E Committee
- International Collaboration (UK/Europe)
- Cross Linking with Other IDPV Efforts
  - BBFA, ISO 29115, ITU-T, ABA
- **New Participants**
  - USPS, AAMVA, CBN, DHS (Policy Office)

2. Consideration Being Given to **Change of Scope & Anticipated Delivery Dates** as Part of T & E and Success Assurance

3. Consideration Being Given to **Development of Methodology for Requirements Specification**



## EXHIBIT 7 – Introduction to Workshop 1 ([back to WS1](#))

The scope of this standard development project reads as follows :

***The development of an American national standard and implementation guidelines for identity proofing processes, verification processes and requirements for information to be used in support of identity establishment for end users and relying parties.***

In summary we must develop:

- a) proof and verification processes**
- b) requirements for information (evidence) to support identity establishment**
- c) implementation guidelines for a) and b)**



**Cause**

**Specification of Requirements for Information**

**Need a Methodology to do this**

**Effect**

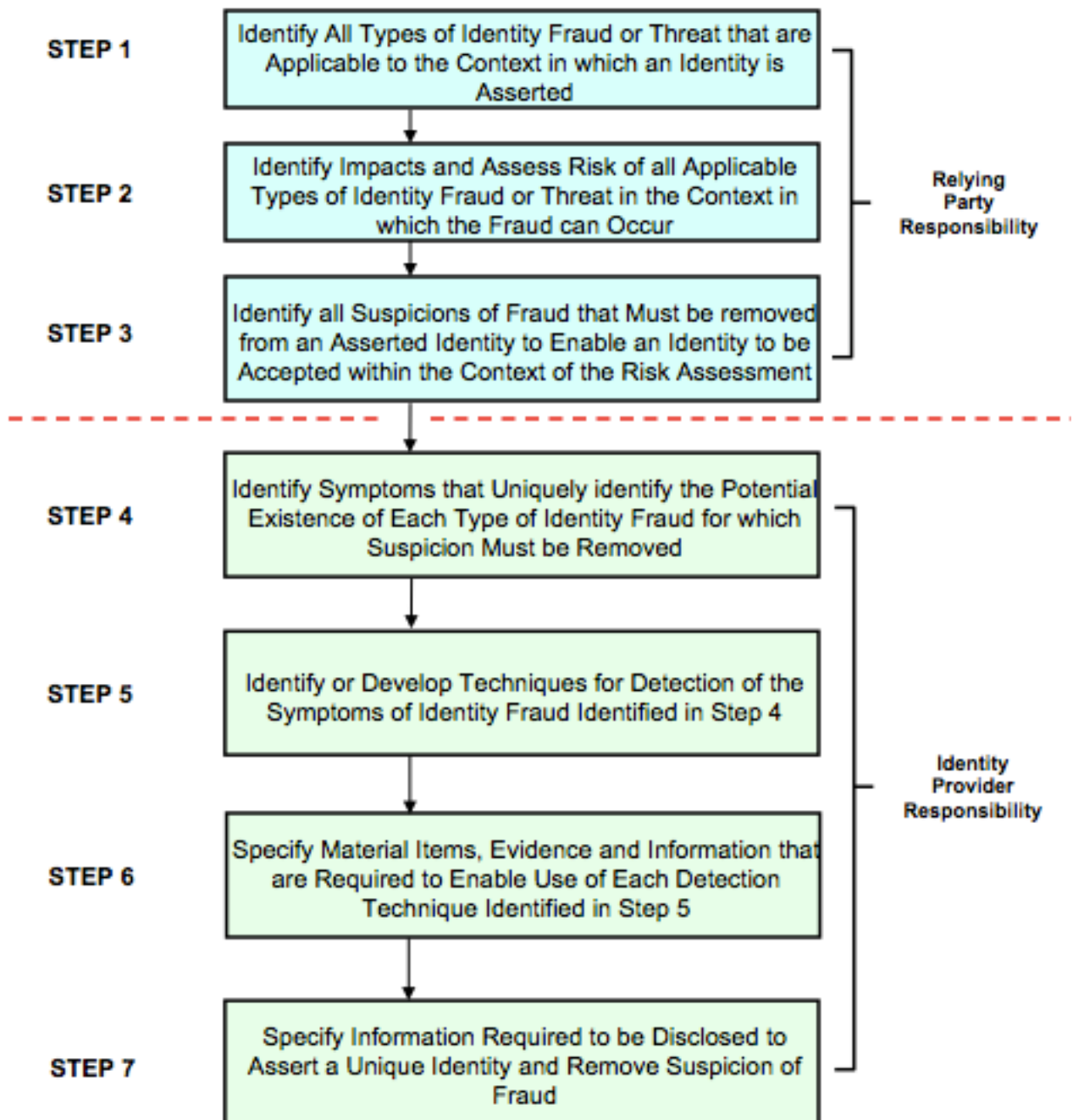
**Specification of Proof and Verification Processes**

**Need a Process to Acquire & Use Information**



## IDPV Framework Part 1 [\(Back to Workshop 1 Report\)](#)

Specification of Information Required  
for the  
Establishment of Identity





# Purpose of Workshop 1

To Propose and Assess Viability of a Methodology for the Specification of Requirements for Information to be Used in support of Identity Establishment for End Users and Relying Parties

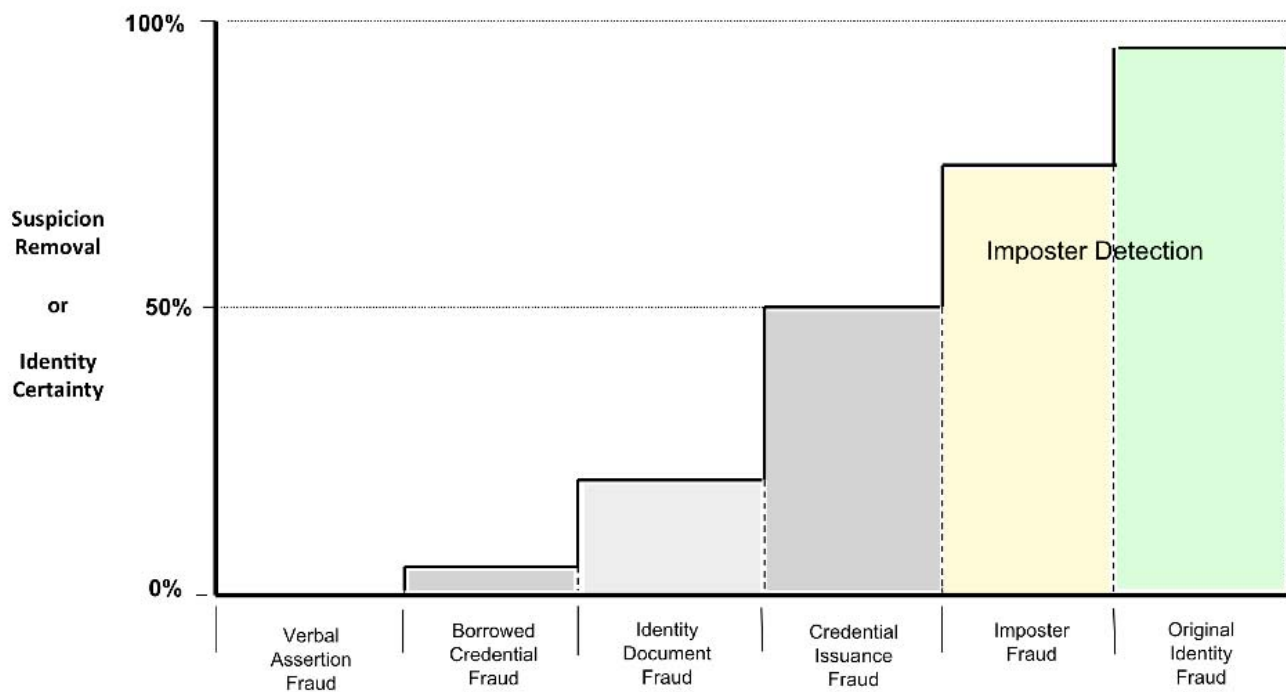


## Anticipated Outcomes of Workshop 1

1. Understanding of the **Reasons** for Developing a Methodology
2. Clear Understanding of the Proposed Methodology – Its' Strengths & Weaknesses
3. A Critique of the Methodology
4. Consensus on the Viability of the Proposed Methodology
5. Recommendations for Development & Testing of the Proposed Methodology



## The Concept of Removal of Suspicion of Types of Identity Fraud





## **Reasons for Development of an IDPV Methodology**

- 1.** Need for “Suspicion Removal” Must be Closely Linked to Unique Identity Risk Circumstances
- 2.** Specifying Requirements of this Kind Must Avoid Subjectivity as much as Possible
- 3.** Use of a Specified Methodology Standardizes the Requirement Specification Process Leading to Greater Understanding and Repeatability
- 4.** Credibility of IDPV Consensus Body/Standard will be Impacted if Identity Assurance Requirements Lack the Use of a Sound Methodology
- 5.** Provides a Reasoned Basis for Accepting the Suspicion of Specific Types of Fraud



## Summary of Part 1 of the proposed IDPV Framework

- A Top Down Identity Risk Management Approach
- Focused on the **Context** in which Identity Risk is Being Taken
- Assesses the **Impact of Accepting a False Assertion** of Identity by Addressing All Applicable forms of Identity Fraud or Threat
- Establishes the Symptoms of Fraud for which Suspicion Must be Removed
- Uses the Established Symptoms to Select or Develop Fraud Detection Techniques
- Detection Techniques Determine the Requirements for Information and/or Other Forms of Evidence to be Obtained from the Person Asserting the Identity



**EXHIBIT 8 – Workshop 1 Worksheets** ([Back to Report](#))

**Sheet 1 – The 6 OMB-04-04 Impact Categories Used in Workshop 1**

Table 1 – Maximum Potential Impacts for Each Assurance Level

<b>Potential Impact Categories for Authentication Errors</b>	<b>Assurance Level Impact Profiles</b>			
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High



## Sheet 2 – Methodology for the Specification of Information Requirements

1. Identify Relevant Types of Identity Fraud/Threat
2. Identify All Credible Impacts of Identity Fraud listed in 1 above
3. Assess Impacts of Fraud - None, Low, Moderate, High
4. For All Impacts, Assessed High, Identify Symptoms of Fraud
5. Specify Detection Technique for symptoms of High Fraud Impact
6. Specify Evidence/Information Required to Enable Detection Techniques
7. Specify Information to be Disclosed to Assert Unique Identity (This step may be unnecessary if this information is required to satisfy Step 6)



### Sheet 3 – Step 1 of the Process

## Identify relevant types of identity fraud/threat

<b>Ref No.</b>	<b>Fraud or Threat Type</b>	<b>Relevant to Context (Y/N)</b>
<b>1</b>	<b>Verbal Assertion Fraud</b>	
<b>2</b>	<b>Borrowed Credential Fraud</b>	
<b>3</b>	<b>Identity Document Fraud</b>	
<b>4</b>	<b>Credential Issuance Fraud</b>	
<b>5</b>	<b>Imposter Fraud</b>	
<b>6</b>	<b>Original Identity Fraud</b>	



**Sheet 4 – Step 2 of the Process (pre set from Sheet 1)**

**Identify all credible potential impacts of identity fraud listed  
in Step**

<b>Ref No.</b>	<b>Potential Impact Areas</b>
<b>1</b>	<b>Inconvenience, distress, or damage to standing or reputation</b>
<b>2</b>	<b>Financial loss or organization liability</b>
<b>3</b>	<b>Harm to organizations programs or public interest</b>
<b>4</b>	<b>Unauthorized disclosure of sensitive information</b>
<b>5</b>	<b>Personal Safety</b>
<b>6</b>	<b>Civil or criminal violations</b>



**Sheet 5 – Step 3 of the Process  
(to be completed by workshop participants)**

**Assess Potential Impact of Fraud as : none or n/a, L, M or H**

Ref No.	Identity Fraud or Threat Types Relevant to the Context	Areas of Potential Impact					
		Inconvenience, distress or damage to standing or reputation	Financial loss or organization liability	Harm to organization programs or public interests	Unauthorized disclosure of sensitive information	Personal Safety	Civil or criminal violations
		1	2	3	4	5	6
1	Verbal Assertion Fraud						
2	Borrowed Credential Fraud						
3	Identity Document Fraud						
4	Credential Issuance Fraud						
5	Imposter Fraud						
6	Original Identity Fraud						



**Sheet 5 – Steps 4, 5 and 6 of the Process  
(to be completed by workshop participants)**

**Identify Fraud Symptoms, Detection Techniques and Evidence/  
Information that will Enable Detection**

<b>Ref No.</b>	<b>Fraud or Threat Type</b>	<b>Symptoms</b>	<b>Detection Techniques</b>	<b>Evidence or Information Required for Detection</b>
1	Verbal Assertion Fraud			
2	Borrowed Credential Fraud			
3	Identity Document Fraud			
4	Credential Issuance Fraud			
5	Imposter Fraud			
6	Original Identity Fraud			



## Sheet 6 – Step 7 of the Process

### Identify the Minimum Information Required to Assert a Unique Identity and Remove Suspicion

Ref No.	Fraud or Threat Type	Personally Identifiable Information (PII)
1	Verbal Assertion Fraud	
2	Borrowed Credential Fraud	
3	Identity Document Fraud	
4	Credential Issuance Fraud	
5	Imposter Fraud	
6	Original Identity Fraud	



## EXHIBIT 9 – Slides Presented by Kim Little ([Jump Back](#))

### Slide 1 – Key Points from our Splinter Group Discussion

- Our consensus body needs to have a deliberate understanding that we are shifting much of the activity from “positive identification” to “negative identification” or “removal of suspicion”
- The methodology needs to not just be for internal use, but for the users of our standard
- Recommended modifications to the proposed methodology

### Slide 2 – Positive Identification Defined

1. Evidence proving that you are who you say you are;
2. Evidence establishing that you are among the group of people already known to the system; recognition by the system leads to acceptance; “A system for positive identification can prevent the use of a single identity by several people”

### Slide 3 – Negative Identification Defined

#### “Removal of Suspicion”

1. Evidence proving that you are not who you say you are not.
2. Evidence establishing that you are not among a group of people already known to the system. Recognition by the system leads to rejection.  
“A system for negative identification can prevent the wrongful or multiple use of identities by a single person”

### Slide 4 – Proposed Methodology

1. Identify Relevant Types of Identity Fraud/Threat
2. Identify All Credible Impacts of Identity Fraud listed in 1 above
3. Assess Impacts of Fraud - None, Low, Moderate, High
4. For All Impacts, Assessed High, Identify Symptoms of Fraud
5. Specify Detection Technique for symptoms of High Fraud Impact



6. Specify Evidence/Information Required to Enable Detection Techniques
7. Specify Information to be Disclosed to Assert Unique Identity (**This step may be unnecessary if this information is required to satisfy Step 6**)

### **Slide 5 – Recommendations to Amend the Proposed Methodology**

1. Identify relevant types of identity fraud/threat.
2. Identify all credible impacts of identity fraud listed and assess impacts of fraud (none, low, moderate, high).
3. For all relevant types of identity fraud, identify the symptoms and method of detection.
4. Specify the mitigation strategy to resolve the relevant types of identity fraud.
5. Specify the information required (to be disclosed) to assert a unique identity and remove suspicion of fraud.
6. Specify tools for validating information.

### **Slide 6 – Revisions to Proposed Methodology**

1. Identify Relevant Types of Identity Fraud/Threat
2. Identify All Credible Impacts of Identity Fraud listed in 1 above
3. Assess Impacts of Fraud - None, Low, Moderate, High

Revision: combine 2 and 3

2. Identify all credible impacts of identity fraud listed and assess impacts of fraud (none, low, moderate, high).

### **Slide 7 – Further Revisions**

4. For All Impacts, Assessed High, Identify Symptoms of Fraud

Revision:

3. For all relevant types of identity fraud, identify the symptoms and method of detection.



**Slide 8 – Further Revisions**

**5. Specify Detection Technique for symptoms of High Fraud Impact**

**Revision:**

**4. Specify the mitigation strategy to resolve the relevant types of identity fraud.**

**Slide 9 – Further Revisions**

**6. Specify Evidence/Information Required to Enable Detection Techniques**

**Revision: Remove**

**7. Specify Information to be Disclosed to Assert Unique Identity**

**Revision:**

**8. Specify tools for validating information.**



**Slide 10 – Further Revisions – Modify Sheet 5, Step 3 of the Process**

Ref No.	Techniques	Outcome			
		Legitimate	False Negative	Imposter Fraud	Original Identity <i>(Synthetic Identity)</i>
		A	B	C	D
1	Verbal Assertion				
2	Borrowed Credential				
3	Altered Document				
4	Identity Document				
5					
6					

[\(Back to Top\)](#)